# Aula 04

## O CONCEITO DE GRUPO

### META

Apresentar o conceito de grupo, as primeiras definições e diversos exemplos.

### OBJETIVOS

Definir e exemplificar grupos e subgrupos.

Aplicar as propriedades dos grupos na resolução de problemas.

Reconhecer grupo cíclico.

Reconhecer o grupo de permutações e seus subgrupos.

### PRÉ-REQUISITO

O curso de Fundamentos de Matemática e as propriedades dos números inteiros estudados nas aulas anteriores.

## INTRODUÇÃO

Estamos de volta para mais uma aula. Esperamos que você tenha gostado do conteúdo estudado nas três aulas anteriores. Nesta aula, vamos começar de fato o que é conhecido como Álgebra abstrata.

A teoria dos grupos embora tenha sido inicialmente estudada por matemáticos, no inicio do século XX os físicos usando argumentos desta teoria fizeram descobertas importantes sobre a estrutura dos átomos e das moléculas em Mecânica Quântica.

Hoje a teoria dos grupos é aplicável em outras áreas tanto das ciências afins quanto em outras da Matemática.

Dentro das estruturas algébricas, os grupos têm uma das estruturas mais simples e, portanto, mais geral. Vamos em frente!

## CONCEITO DE GRUPO

Definição 1. Definimos grupo como sendo todo par $(G,\cdot)$ onde $G$ é um conjunto não vazio e $\cdot$ é uma operação binária em $G$ verificando às seguintes propriedades.

i)Associativa, $\forall a,b,c \in G, (a\cdot b)\cdot c = a\cdot(b\cdot c)$.

ii) Existência do elemento identidade. Existe $e \in G$ tal que $a\cdot e = e\cdot a = a$.

iii) existência do inverso. Para cada $a \in G$, existe $b \in G$ tal que $a\cdot b = b\cdot a = e$.

Em geral, com o intuito de simplificar notação escrevemos apenas $G$ em vez de $(G,\cdot)$.

Se $e$ e $e^{'}$ são elementos identidades de um grupo, então $e^{'} = e\cdot e^{'} = e$ donde podemos concluir que o elemento identidade é único.

Para cada elemento a, num grupo $G$, se existem $b$ e $c$ no grupo inversos de $a$, então $b = b\cdot e = b\cdot(a\cdot c) = (ba)\cdot c = c$.

Donde temos também que o inverso de cada elemento $a \in G$ é único. Denotamos o inverso de $a$ por $a^{-1}$.

Quando num grupo $G$ além das três propriedades exibidas na definição se unifica a propriedade:

iv)$\forall\ a,b \in G,\ \ a\cdot b = b\cdot a$, dizemos que $(G,\cdot)$ é abcliano (ou comutativo).

Quando a operação for uma adição (simbolizada por +) dizemos que $(G, +)$ é um grupo aditivo. Neste caso indicamos a identidade por "$0$" e o inverso de cada $a \in G$ por $-a$. Os grupos aditivos são sempre abelianos.

Quando o conjunto $G$ é finito, dizemos que $(G,\cdot)$ é um grupo finito, no caso contrário dizemos que $(G,\cdot)$ é um grupo infinito.

Definição 4.2.2. Definimos a ordem de um grupo $(G,\cdot)$ como sendo a cardinalidade do conjunto $G$. Indicamos: $|G|$.

Obviamente, temos grupos finitos (nestes a ordem é um inteiro positivo) e grupos infinitos.

Exemplo 1. $(\mathbb{Z}, +)$ é um grupo aditivo infinito

Exemplo 2. $G = \{\mathfrak{z} \in \mathbb{C}; |\mathfrak{z}| = 1\}$, $(G,\cdot)$ é um grupo abeliano infinito

Exemplo 3. Seja $(G = \{1, -1\},\cdot)$ onde $1 \cdot 1 = -1 \cdot (-1) = 1$ e $1 \cdot (-1) = -1 \cdot 1 = -1$. Então $G$ é um grupo abcliano finito com apenas dois elementos, $i.é$, $|G| = 2$.

Exemplo 4. O subconjuntos dos números complexos $G = \{1, i, -1, -i\}$ onde $i$ é a unidade imaginária, cuja operação é a restrição da multiplicação de $G$ a este conjunto é um grupo finito com quatro elementos, ou seja, $|G| = 4$

Exemplo 5. Seja $G$ o conjunto das matrizes quadradas de ordem $n$ com entradas em $\mathbb{Z}$. Então $(G, +)$ é um grupo abeliano.

Exemplo 6. Seja $G = Gl_n(\mathbb{R})$ o conjunto das matrizes quadradas de ordem $n$ não-singulares de entradas reais. Este conjunto munido da restrição do produto usual de matrizes é um exemplo de grupo não abeliano infinito.

Exemplo 7. Sejam $n \in \{2,3,4, \dots\}$ e $G = \{\mathfrak{z} \in \mathbb{C}; \mathfrak{z}^n = 1\}$. Então $G$ munido da restrição de produto de números complexos é um grupo abeliano finito contido $n$ elementos.

Exemplo 8. Sejam $S$ um conjunto não vazio e $G$ o conjunto de todas as funções bijetivas $f: S \longrightarrow S$. Então $G$ munido da composição de funções é um grupo, chamado grupo das permutações de $G$. Em particular, quando $S = \{1,2, \dots, n\}$, $G$ é chamado o grupo das permutações de nível $n$ tem ordem $n!$ e o indicamos por $S_n$. Este grupo desempenha um papel importante na teoria dos grupos finitos, como veremos futuramente.

Proposição 1. (Propriedades imediatas de um grupo)

i) A identidade é única.

ii) O inverso de cada elemento é único.

iii) Se $a, b, c \in G$ e $a.c = b.c$ então $a = b$.

iv) Se $a.a = a$ então $a = e$

v) A equação $ax = b$ tem como solução única $x = a^{-1}.b$.

Demonstração: i) Seja $G$ um grupo e suponhamos que existam $e, e' \in G$ tais que $a.e = e.a = a$ e $a.e' = e'.a = e' \ \forall\, a \in G$. Em particular $e' = e'.e = e.e' = e$.

ii) Seja a um elemento de $G$ e suponhamos que existam $b, c \in G$ tais que $a.b = b.a = a.c = c.a = e$. Então, $c = c.e = c.(a.b) = (c.a).b = e.b = b$.

iii) Como $a.c = b.c$, da unicidade do inverso, temos que $(a.c).c^{-1} = (b.c).c^{-1} \Rightarrow a.(c.c^{-1}) \Rightarrow a.e = b.e \Rightarrow a = b$.

iv) $a.a = a \ \Rightarrow (a.a).a^{-1} = a.a^{-1} \Rightarrow a.(a.a^{-1}) = a.a^{-1} \Rightarrow a = e$.

v) $ax = \ b \Rightarrow a^{-1}(ax) = a^{-1}.b \Rightarrow (a^{-1}.a)x = a^{-1}.b \Rightarrow e.x = a^{-1}.b \Rightarrow x = a^{-1}.b$. (A unicidade do inverso garante a unicidade da solução).

Definição 3. Dados um grupo $G$ e $a_1, a_2, \dots, a_n \in G$, definimos o produto destes elementos nesta ordem, indutivamente, como segue: $a_1.a_2 \dots .a_n = (a_1.a_2 \dots .a_{n-1}).a_n$.

Se $j \in \{1,2,3, \dots, n-1\}$, pode-se provar que $\left(a_1.a_2 \dots .a_j\right).\left(a_{j+1} \dots .a_n\right) = a_1.a_2 \dots .a_n$.

Definição 4. Dados $G$ grupo, $a \in G$ e $n \in \mathbb{Z}$, definimos a potência de base $a$ e expoente $n$ como sendo

$$a^n = \begin{cases} e \ se \ n = 0 \\ a^{n-1}.a \ se \ n \geq 1 \\ (a^{-1})^{-n} \ \ se \ \ n \leq -1. \end{cases}$$

Usando indução, podemos provar que $\forall\, a \in G$ e$\forall\, m, n \in \mathbb{Z}$, valem

i)$a^m.a^n = a^{m+n}$

ii)$(a^m)^n = a^{m.n}$.

Definição 5. Sejam $G$ um grupo e $H$ um subconjunto não vazio de $G$. Dizemos que $H$ é um subgrupo de $G$ se $H$ munido da restrição $a$ si da operação de $G$ é também um grupo.

Da unicidade do elemento identidade e da necessidade da existência deste elemento num grupo segue que a identidade de $G$ pertence a $H$.

Uma condição necessária e suficiente para que um subconjunto $H$ de $G$ seja um grupo é que i) $H \neq \phi$ e ii)$\forall a, b \in H$ se tenha $ab^{-1} \in H$.

Notemos que as duas condições acima são verificadas por todo grupo e, se $H \subset G$ e $H$ verifica i e ii, então, dado $a \in H$, $e = a.a^{-1} \in H$ e, dados $a, b \in H$, $b^{-1} = e.b^{-1} \in H \Longrightarrow x, b^{-1} \in H \Longrightarrow a.(b^{-1})^{-1} = a.b \in H$. A associatividade da restrição da operação de $G$ a $H$ em $H$ é óbvia.

Quando $H$ é subgrupo de $G$ indicamos por $H \leq G$.

Exemplo 10. Seja $(G = \{1, i, -1, -i\}, .)$. então $(H = \{1, -1\}, .)$ é um subgrupo de $G$. $(H \leq G)$.

Exemplo 11. $(G = \{z \in \mathbb{C}; |z| = 1\}, .)$ e $H = \{z \in \mathbb{C};\ z^3 = 1\}$. Então $H \leq G$.

Exemplo 12. Seja $G$ um grupo e $H = \{a \in G;\ \ ax = xa, \forall x \in G\}$. Então, $H \leq G$. Notamos que $e \in H$, pois em $G$, $e$ comuta com todos os elementos de $G$. Segue que $e \in H$ e $H \neq \phi$. Sejam $a, b \in H$. Então $(ab^{-1})x = a(b^{-1}x) = (b^{-1}x)a = b^{-1}(xa) = b^{-1}(ax) = (b^{-1}a)x = (ab^{-1})x \Longrightarrow ab^{-1} \in H \Longrightarrow H \leq G$.

Para cada $G$, o subconjunto formado pelos elementos que comutam com todos os elementos de $G$ é chamado o centro de $G$ e o indicamos por $Z(G)$.

Observemos que quando $G$ é abeliano $Z(G) = G$.

Exemplo 13. Sejam $G$ um grupo e $a \in G$. Seja $H = \{x \in G; xa = ax\}$. Então $\forall\ x \in Z(G), x \in H$, ou seja, $Z(G) \subset H$ e $H \neq \phi$. Se $c, d \in H$ então $ad = da\ \Longrightarrow d^{-1}a = ad^{-1} \Longrightarrow d^{-1} \in H$ . Portanto, $(cd^{-1}).a = c(d^{-1}a) = c(ad^{-1} = (ca).d^{-1} = a.(cd^{-1}) \Longrightarrow cd^{-1} \in H$ e $H \leq G$. Este subgrupo de $G$ é chamado o centralizador de $a$ em $G$ e o indicamos por $C_G(a)$. Notamos que $\forall a \in G, Z(G) \leq C_G(a)$.

Exemplo 14. $G = Gl_n(\mathbb{R})$ e $H = GL_n(\mathbb{Q})$ então $H \leq G$.

Definição 6. Seja $G$ um grupo. Dizemos que $G$ é cíclico se existe um elemento $a \in G$ tal que $G = \{a^n; n \in \mathbb{Z}\}$. Dizemos também que $G$ é gerado por $a$ e indicamos $G =< a >$.

Exemplo 15. Seja $z = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} \in \mathbb{C}$.

Então $G =< z >= \{1, z, z^2\} = \{z^n; n \in \mathbb{Z}\}$ é cíclico finito de ordem 3. Notemos que dado $n \in \mathbb{Z}$, do algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que $n = 3q + r$ e $r \in \{0,1,2\}$. Logo $z^n = \cos\frac{2n\pi}{3} + i\sin\frac{2n\pi}{3} = \cos(\frac{2r\pi}{3}) + i\sin\frac{2r\pi}{3} \Longrightarrow z^n \in \{1, z, z^2\}$.

Exemplo 16. Dados $G$ grupo e $a \in G$, o conjunto $H =< a >= \{a^m; m \in \mathbb{Z}\}$ é um grupo cíclico de $G$. Notemos que $a^0 = e \in H$. Se $x = a^m \in H$ então $xy^{-1} = a^m.(a^n)^{-1} = a^{m-n} \in H$.

Observação. Quando um grupo é aditivo, a potência de base $a$ e expoente $n$ é denotada por $na$.

Exemplo 17. O grupo $(\mathbb{Z}, +)$ é cíclico infinito gerado por 1.

$\mathbb{Z} = \{\dots, -2, -1,0,1,2,3, \dots\} = \{n.1; n \in \mathbb{Z}\}$. O conjunto $H = \{\dots, -4, -2,0,2,4, \dots\} = \{2n; n \in \mathbb{Z}\}$ é o subgrupo cíclico de $\mathbb{Z}$ gerado pelo elemento 2. Então podem escrever: $\mathbb{Z} =< 1 >$ e $H =< 2 >$.

Observação. Notemos que se $G$ é cíclico gerado pelo elemento $a$ e $x = a^m, y = a^n \in G$ então $xy = a^m . a^n = a^{m+n} = a^{n+m} = a^n . a^m = y.x$, portanto $G$ é abeliano.

Proposição 2. Todo subgrupo de um grupo cíclico é cíclico.

Demonstração: Sejam $G =< a >$ cíclico e $H \subset G$. Se $H = \{e\}$ ok! Pois $H =< e >$. Se $H \neq \{e\}$, então, o conjunto $A = \{m \in \mathbb{Z}_+^*, a^m \in H\}$ é não vazio. Sejam $d = minA$ e $b = a^d \in H$.

Afirmamos: $H =< b >$. De fato, pois se $x = a^m \in H$ então, do algoritmo da divisão existem $q, r \in \mathbb{Z}$ tais que $a^m = a^{dq+r}$ e $0 \leq r < d$. Segue que $a^r = a^{m-dq} \in H$. Mas, da minimalidade de $d$ segue que $r = 0 \Longrightarrow x = a^m = (a^d)^q = b^q \in< b >\Longrightarrow H \subset< b >$. Como $b \in H, \forall n \in \mathbb{Z},\ b^n \in H \Longrightarrow< b >\subset H$ e $H =< b >$.

## RESUMO

Caro aluno, nesta aula, nós estabelecemos o conceito de grupo, onde definimos grupos e subgrupos apresentamos diversos exemplos, apresentamos os subgrupos especiais centro e centralizador de um elemento num grupo e grupos cíclicos.

## ATIVIDADES

1. Seja $G$ um grupo abeliano. Prove que se $a, b \in G$ e $m \in \mathbb{Z}$, então $(ab)^m = a^m . b^m$.

2. Seja $G$ um grupo e suponha que $a^2 = e, \forall a \in G$. Prove que $G$ é abeliano.

3. Seja $G$ um grupo e $a, b \in G$. Prove que $(ab)^{-1} = b^{-1}. a^{-1}$.

4. Seja $p \in \mathbb{Z}_+$ um primo, prove que $G = \mathbb{Z}_p \backslash \{\bar{0}\}$ é um grupo abeliano com $p - 1$ elementos.

5. Se $G$ é um grupo finito de ordem par. Prove que existe $a \in G \backslash \{e\}$ tal que $a^2 = l$

6. Sejam $G = gl_2(\mathbb{R})$ e $H$ o subconjunto de $G$ formado pelas matrizes anti-simétricas. Prove que $H \leq G$.

7. Sejam $G_1, G_2$ grupos e seja $G = G_1 X G_2$. Defina uma operação em $G$ do seguinte modo:

$(a_1, b_1), (a_2, b_2') \in G \Longrightarrow (a_1, b_1).(a_2, b_2) = (a_1 a_2, b_1 b_2)$. Prove que $(G,\cdot)$ é um grupo. Este grupo é chamado produto direto de $G_1$ e $G_2$. Se $H = \{(e, b); b \in G_2\}$, prove que $H \leq G$.

8. Prove que todo grupo $G \neq \{e\}$ tem um subgrupo cíclico $H, H \neq \{e\}$.

9. Seja $G = S_n$. Indicando cada elemento $\sigma \in S_n$ do seguinte modo,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Escreva explicitamente o grupo $S_3$. Calcule $Z(S_3)$ e conclua que $S_3$ não é abeliano.

10. Prove que o subconjunto $H$ de $S_4$ dos elementos $\sigma$ tais que $\sigma(4) = 4$ é um subgrupo de $S_4$.

11. Se $L$ e $H$ são subgrupo de um grupo $G$, prove que $L \cap H$ é um subgrupo de $G$ e que , em ral $L \cup H$ não é subgrupo de $G$.

## COMENTÁRIO DAS ATIVIDADES

Caro aluno, se você fez as cinco primeiras atividades então entendeu as propriedades dos grupos.

Na segunda atividade você deve ter notado que $a^2 = e \Leftrightarrow a = a^{-1}$ e usado o fato de que $(ab)^{-1} = b^{-1}.a^{-1}$.

Na terceira, você deve ter multiplicado $ab$ por $b^{-1}.a^{-1}$ pela esquerda e pela direita e usado o fato de que o inverso de um elemento num grupo é único.

Na quinta atividade, você deve ter notado que todo elemento tem um único inverso e que a identidade tem como inverso ela própria.

Nas sete ultimas atividades exploramos a definição de subgrupo. Se você compreendeu esta definição não deve ter tido dificuldades, hesitou possivelmente na última questão onde você deve ter notado que $L \cup G$ é subgrupo se, e somente se, $L \subset H$ ou $H \subset L$. Lembre-se de que o objetivo das atividades é fixar os conteúdos desenvolvidos na aula. Portanto você deve ler estes conteúdos com carinho quantas vezes sejam necessárias. Lembre-se também que a ajuda dos tutores é importante.

## REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de algebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).